CATO
NETWORKS

SASE In Manufacturing

A Response to the Challenges of Industry 4.0

The Double-Edged Sword
of the Fourth Industrial Revolution

Industry 4.0 has brought significant change to the manufacturing industry. Driven by technological advancements, changing consumer demands, and global competition, the emergence of smart factories has propelled manufacturing into a more digitized, connected, and automated era.

Artificial intelligence (AI), the Internet of Things (IoT), and robotic process automation (RPA) are becoming more prevalent on the factory floor, revolutionizing how products are designed, produced, and distributed. While these advancements offer the potential for improvements such as streamlined operations, efficiency, predictive insights, and overall process optimization, they also create new challenges that manufacturers must navigate to harness the benefits of digital transformation.

Contact Us

Network Security

Traditional manufacturing machinery, systems, and devices were not engineered with today's cyber threats in mind. This leaves them exposed and vulnerable to increasingly sophisticated attacks. As manufacturing processes become more reliant on technology and interconnected devices, the likelihood of cyber-attacks increases. Threat actors can exploit vulnerabilities in these systems, leading to operational disruption, theft of sensitive and proprietary data, or even physical damage to critical equipment. The pace of technological innovation often outpaces the ability of manufacturers to update and secure their assets, further increasing security risks.

Global Connectivity and Network Performance

The reliance on outdated legacy network solutions like MPLS presents hurdles in addressing the global connectivity needs of manufacturers, especially in remote locations or regions. Flexibility and scalability are needed as manufacturers seek to integrate cloud-based applications and services into their operations to support highly distributed environments and deliver better user experiences. Data volumes generated by connected devices can overwhelm traditional network architectures. As manufacturers depend on real-time data for decision-making, delays in data transfer and processing can have negative consequences. A network that prioritizes critical data while maintaining high performance means manufacturers stay competitive.

High Operational Costs

The complexity and financial burden of managing and maintaining disparate network and security point solutions increases operational costs, posing significant obstacles to achieving the agility and efficiency manufacturing envisioned with Industry 4.0. An adaptable, agile and cost-effective network that can respond swiftly to business needs is needed to align strategic initiatives with IT investments

IT Resource Constraints

Manufacturers often struggle to balance the need for new technology with limited IT resources. In some sectors, tight budgets and lower profit margins mean resources get cut, resulting in lean IT teams compared to the number of users they serve. These teams spend most of their time managing and maintaining complex legacy infrastructures instead of focusing on strategic goals or developing new skills that drive innovation. Rapid technology evolution makes things even tougher, increasing the pressure on already stretched IT resources and widening the skills gap. This makes it hard for IT to support the business effectively.

Caught in a catch-22, these challenges hinder company growth and weaken competitive edge.
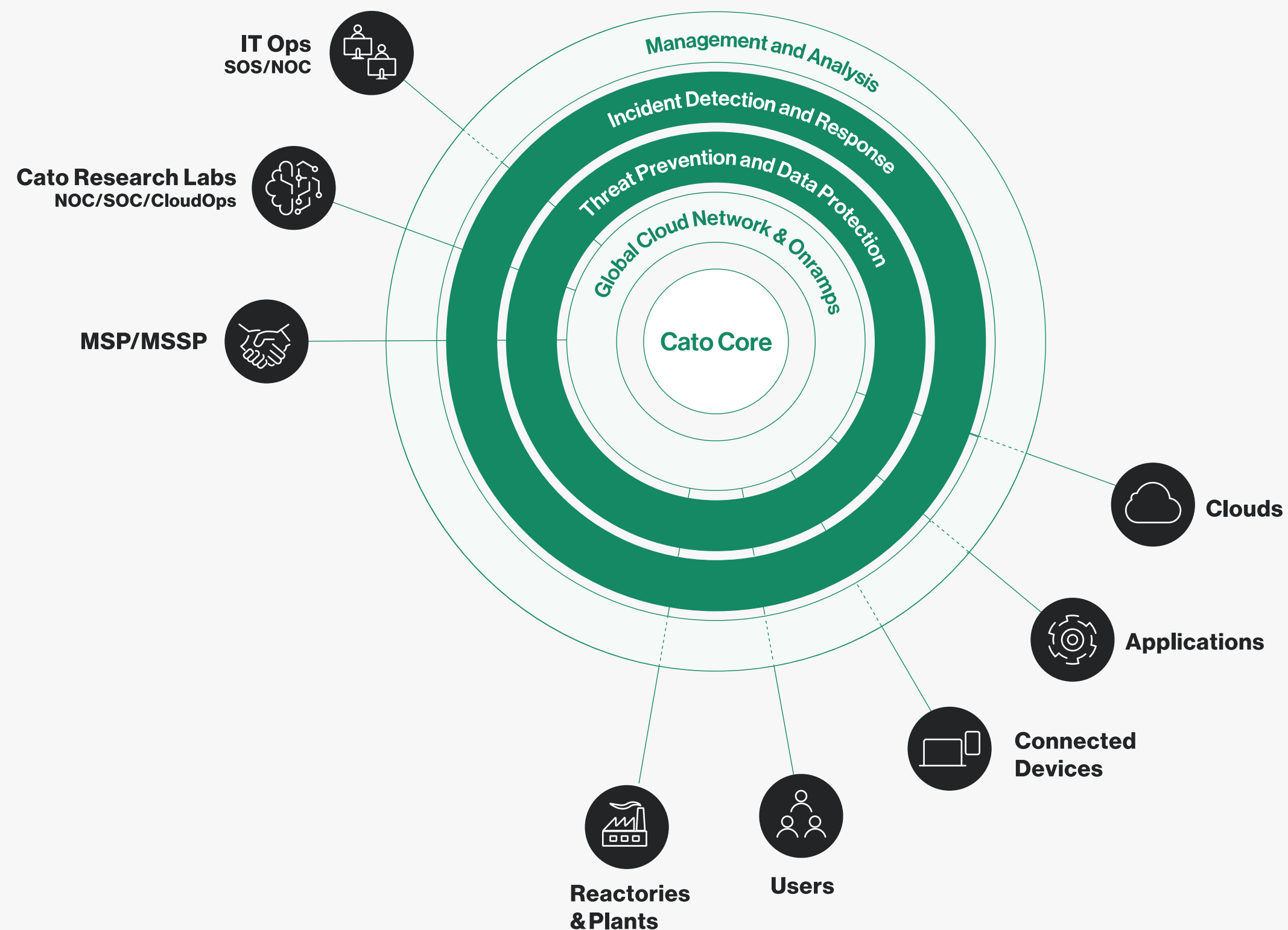
# SASE: Fortifying and Simplifying Manufacturing in Industry 4.0

Secure Access Service Edge (SASE) is a modern framework that converges networking and security into a single, secure, cloud-based, and globally distributed service. Incorporating a Software-Defined Wide Area Network (SD-WAN) and robust security features like Firewall-as-a-Service (FWaaS), Zero-Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), and Secure Web Gateway (SWG), SASE offers manufacturers an opportunity to streamline IT, shedding the complexities and costs associated with legacy point solution infrastructures.

SASE enhances security posture and reduces the risk of breaches and cyber-attacks. It enables secure access for all users across hybrid work environments, ensures seamless global connectivity, simplified management, and lower costs.

Manufacturers can now focus on the strategic advantages and growth that Industry 4.0 brings, with the simplicity, scalability, and security that SASE provides.

Contact Us

Transformative
Success Stories

How Cato is Changing the Manufacturing Landscape
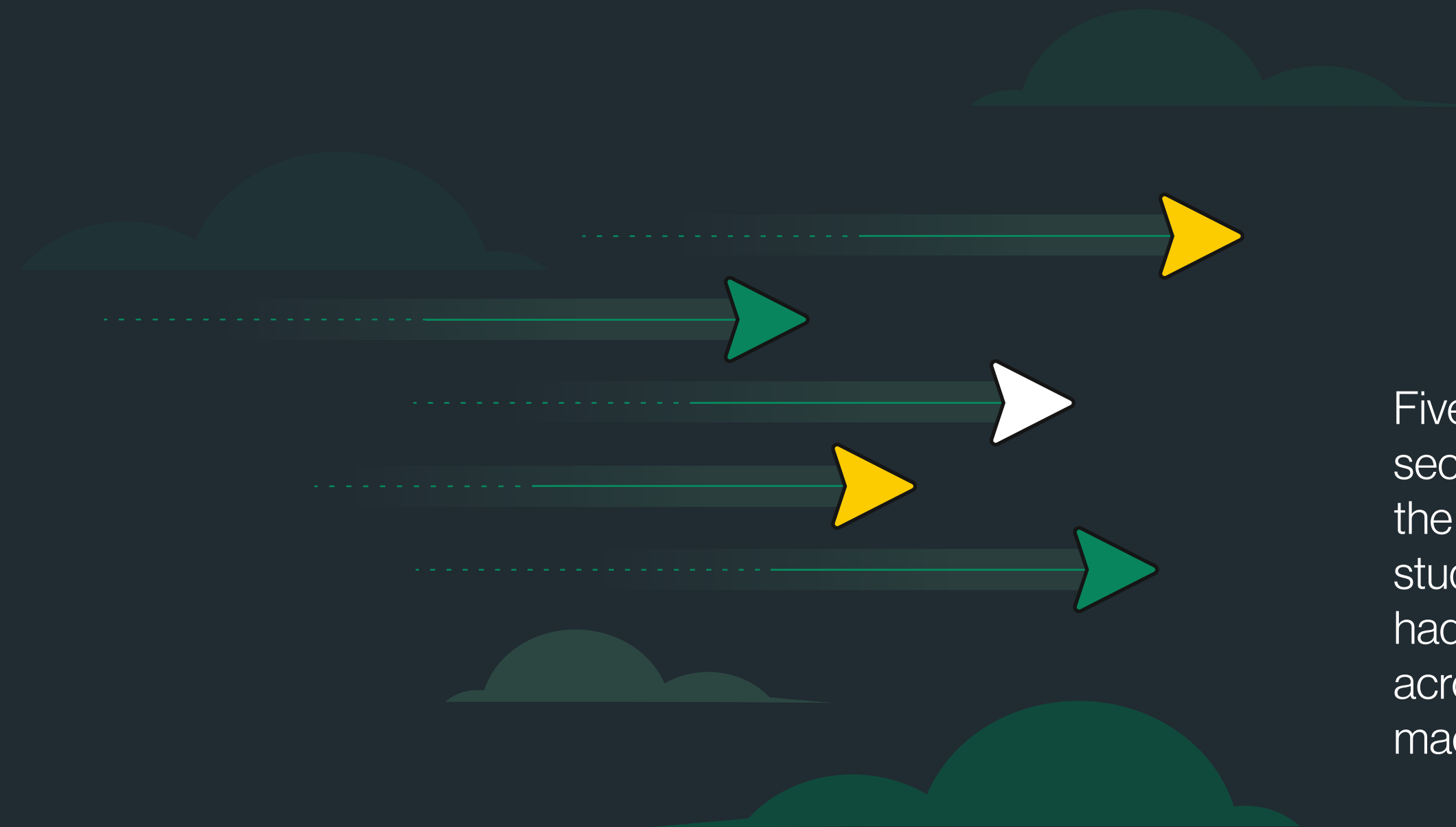
Five global manufacturing leaders overcame their IT security, connectivity, and cost challenges by switching to the Cato SASE Cloud Platform. The following five case studies examine the transformational impact Cato has had on operational effectiveness and business outcomes across manufacturing verticals, including automotive, machinery, and food production.

Contact Us

O-I Taps Augmented Reality and Cato SASE Cloud to Realize "Impossible-to-Count" Savings
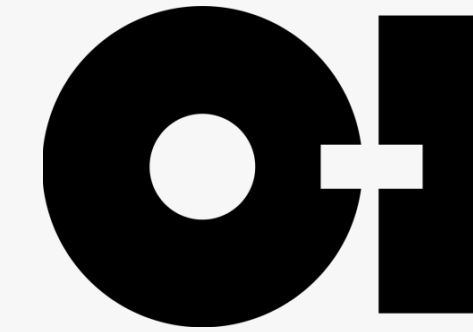
Challenge

O-I faced several IT infrastructure challenges. Its MPLS network was outdated and couldn't meet bandwidth needs in transitioning applications to the cloud. Covid-19 meant thousands of O-I's employees were now working from home, and the existing legacy VPN was unable to support remote user requirements. O-I also needed to enhance security across its global plants. With a small IT team, resources were being drained in maintaining legacy appliances, negatively impacting wider digital transformation initiatives.

Impact and Benefits

O-I quickly saw improvements after implementing Cato SASE Cloud. This included better application performance, facilitating remote work for 24,000 employees, and seamless operation of collaboration tools like Microsoft Teams. Cato's advanced security features provided robust protection across 70 plants in 19 countries, while the introduction of Augmented Reality for remote troubleshooting enhanced operational efficiency. Consolidating networking and security with Cato led to a significant 20% reduction in communication costs.

Solution

O-I put out an RFP to multiple vendors to address its challenges, ultimately selecting Cato after a successful Proof of Concept (PoC). Cato SASE Cloud offered a simple, cost-effective, and quick-to-deploy service compared to other vendors, connecting all enterprise network resources while providing robust security features, enabling I-O to meet its transformation goals.

About

O-I is one of the world's leading producers of sustainable glass containers. O-I partners with global food and beverage companies to transform four basic ingredients into masterfully designed and sustainable glass packaging, helping brands connect with consumers and tell their stories through glass.

Read the full **case study** ⊙

Devro Boosts Network Visibility and Enhances the Hybrid Work Experience with Cato

DEVRO

Challenge

Needing to upgrade their aging firewall appliances to improve global connectivity, especially in remote manufacturing locations, Devro's search for a comprehensive solution led them to explore options beyond legacy firewall vendors.

Impact and Benefits

Devro experienced a non-disruptive, seamless deployment, achieving significant improvements in network connectivity, reliability, visibility, and enhancing the hybrid user experience. They were particularly impressed with the ease of management provided by the Cato Management Application (CMA) for monitoring and troubleshooting. Devro commended Cato's proactive and responsive support team, as well as its commitment to incorporating customer feedback into the Cato SASE Platform.

Solution

Devro determined that Cato was the optimal solution, seamlessly uniting the critical functions they needed with simplified management. Devro selected Cato SASE Cloud for its converged approach, combining SD-WAN and multiple security features into a single, secure, global, cloud-native service. Cato's single pane of glass management was a key differentiator for Devro, introducing simplification and standardization. And, with single sign-on, work from anywhere (WFA) users could bypass daily VPN logins, while allowing IT comprehensive visibility and flexibility to run scans and perform security updates.

About

Devro is a leading global supplier of collagen casings, supporting customers worldwide in making the best sausages possible. With manufacturing sites across Australia, China, Czech Republic, Netherlands, US, and UK, Devro uses its expertise in food science and technology to transform collagen into various casing forms. Committed to innovation, Devro works with customers and distributors to develop new ideas that expand product ranges and market share.

Read the full **case study** ⊙

Vitesco Technologies Builds New Global Enterprise Network with Cato

vitesco TECHNOLOGIES

Challenge

Vitesco Technologies, spun out from Continental AG, faced the challenge of redesigning its global network and security infrastructure from legacy MPLS to better support expansive operations. Vitesco needed a solution that would incorporate its WAN, Internet, and remote access needs effectively. Navigating the 'Great Wall of China' and exiting Office 365 traffic without violating laws was a critical consideration.

Impact and Benefits

Implementing Cato SASE Cloud allowed Vitesco Technologies to achieve high network availability, efficient site setup, and robust threat prevention. Vitesco seamlessly migrated its network infrastructure without downtime, addressing regulatory challenges to ensure compliance with Chinese regulations and enabling seamless access to Office 365. The Cato SASE Cloud platform facilitated self-maintenance, provided deep network analytics, and enforced consistent policies globally, contributing to significant operational improvements.

Solution

Vitesco Technologies chose Cato after evaluating different options with C3 Technology Advisors. Cato SASE Cloud provided a next-gen, converged networking and security solution that would enable Vitesco to set up new sites quickly and efficiently, addressing various critical use cases like supporting users and locations in China, connecting to AWS, ensuring access to special applications, and implementing threat prevention across all traffic. With Cato, a gradual deployment process allowed for smooth migration with minimal downtime.

About

Vitesco specializes in drive technologies, focusing on creating efficient electrification technologies for all types of vehicles. Their portfolio includes 48-volt electrification solutions, electric drives, and power electronics for hybrid and batter-electric vehicles, electronic controls, sensors, actuators, and exhaust after-treatment solutions. Their mission: Powering Clean Mobility.

Read the full **case study** ⊙

The Flügger Group Gains Network Flexibility and Security with Cato and Secher Security

Flügger

Challenge

Flügger Group needed secure, fast WAN connections to facilitate expansion and support over 400 global retail and franchise stores. Despite the security of its MPLS solution, rigidity caused delays in store operations, and managing multiple security point solutions was cumbersome, costly, and time-consuming. Flügger was also modernizing its manufacturing plants, seeking a secure, cost-effective solution to support the needs of its growing network of suppliers and partners.

Impact and Benefits

With Cato, Flügger enhanced its network flexibility and security, streamlining operations, and reducing costs. This shift facilitated easier management of Flügger's expanding retail network making it simple to move, open, and close stores compared to the previous MPLS solution. It also improved Flügger's ability to securely integrate new partners.

Solution

Flügger underwent a network transformation, migrating from MPLS to Cato Edge SD-WAN following a recommendation from its IT security consultant, Secher Security. This move consolidated all WAN and Internet traffic in the cloud with next-gen security capabilities. The implementation involved installing a Cato Socket appliance at each location, providing immediate connectivity to the nearest PoP linked to Cato's global backbone.

About

Flügger Group is a Danish company established in 1783, specializing in the production of high-quality paints and surface treatment products, including decorative paints, wood stains, spackling pastes, wallpapers, and tools. With a rich cultural heritage, Flügger is committed to craftsmanship and excellence, reflected in their quality products and innovative solutions.

Read the full **case study** ⊙

CATO
NETWORKS

Contact Us

Hoyer Motors Taps Cato to Connect China Offices and Cato MDR for Better Malware Protection

HOYER MOTORS

" Our connection is better than what we have ever had, especially in China. We have people in factories in northern China that have never been able to work on remote desktop to connect to our system, and now with Cato, they can do that, and that is really, really big. "

Kenneth Middelboe Carson, IT Senior Administrator

Challenge

Hoyer Motors faced challenges with its network security due to delayed firewall updates from a third-party provider. Updates/patching could take up to 14 days leaving Hoyer's global network vulnerable to malware attack. Add to this a lack of control and no visibility over their firewall appliances, service interruptions at office locations, and a need to migrate to the cloud, a new infrastructure was required.

Impact and Benefits

Hoyer achieved improved global connectivity, particularly in China, where 4G connections in remote areas were now viable. The shift to Cato's SASE platform delivered enhanced security with real-time firewall updates and comprehensive threat detection, reducing the risk of cyberattacks. Hoyer also gained full control over its IT infrastructure, leading to increased productivity and the ability to easily manage and control its network security in-house.

Solution

Hoyer sought a new solution that was easier to manage for IT and worked with Secher Security to explore options. Hoyer opted for a Proof of Concept (PoC) with Cato, initially deploying Cato's edge SD-WAN devices (Cato Sockets), equipping users with the Cato Mobile Client. Branch firewalls were replaced with Cato's security-as-a-service, and Hoyer opted for Cato Managed Threat Detection and Response (MDR) for better malware protection.

About

Hoyer is a leading manufacturer of high-performance electric motors, delivering innovative solutions to a variety of global industries, with a focus on performance, reliability, and sustainability. Hoyer's solutions make it possible for companies to achieve new levels of efficiency and success.

Read the full case study ⊙

CATO NETWORKS

Contact Us

Cato is Highly Rated by Manufacturing Customers on Gartner Peer Insights

Gartner Peer Insights is a platform that enables IT professionals to provide reviews and ratings of various technology products and services. It is an online community where users share their experiences with different vendors and solutions.

Gartner Peer Insights is a valuable resource for businesses when it comes to making decisions about their technology investments. The reviews on the platform come from real users who have firsthand experience with products, ensuring reviews are credible and unbiased.

Cato has over 50 verified user reviews from manufacturers in the Single Vendor SASE category on Gartner Peer Insights – over 10x more than competitors in the space.

Cato SASE Cloud

"Single management console makes for easy security, network and user management across multiple sites and for remote users."

★★★★★

Director OF IT - Manufacturing

Cato SASE Cloud

"Cato is easy to deploy & configure. They also offer a 24X7 NOC that can stop an attack immediately."

★★★★★

Director of Global IT Cybersecurity - Manufacturing

Cato SASE Cloud

"I like the fact that is a cloud solution that is maintained by the vendor."

★★★★★

Engineer - Manufacturing

Cato SASE Cloud Unlocks the Potential of Industry 4.0

With Cato, manufacturers are not just investing in a solution; they're adopting an elegant platform framework that empowers them to take full advantage of the benefits and expectations of Industry 4.0. Cato SASE Cloud enables seamless integration of new technologies, processes, and data into current operations, making it easier to adapt to changing market demands.

As technology advances and production processes become more complex, Cato is equipped to handle these changes and drive efficiencies across the entire value chain. Greater visibility, seamless connectivity, robust security, improved operational effectiveness, and significant cost savings:

SLA-Backed Global Private Backbone:
Points of Presence (PoPs) in remote and rural locations, providing fully encrypted and optimized end-to-end connectivity to any facility, anywhere

Robust Security
Enhanced capabilities like ZTNA to ensure every user and device is verified before gaining access to applications and resources, and FWaaS, SWG, CASB, DLP, RBI, EPP, and XDR to detect, protect, and respond to sophisticated cyber threats

Simplified Management
Single pane of glass management with complete network control and visibility

Flexibility
Agile and adaptable, allowing manufacturers to respond quickly and effectively to business needs

Reduced Complexity and Lower Costs
Removing the burden of deploying, configuring, patching, and maintaining multiple point solutions, reducing operational costs, and improving agility, flexibility, and performance
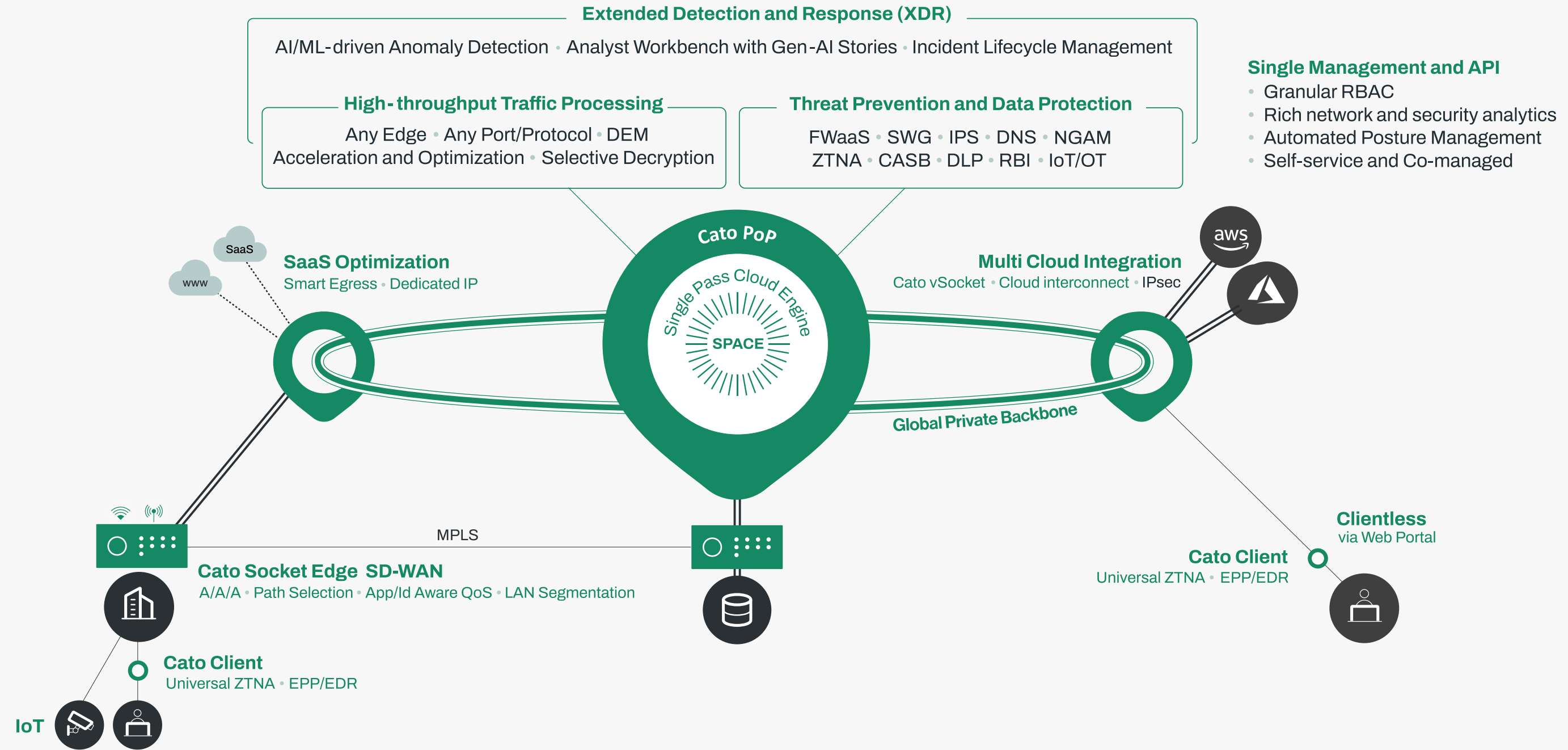
Fast Deployment
Delivered quickly with minimal impact on operations

To learn more about how Cato Networks can help your manufacturing enterprise, start here ⊙

Contact Us

Cato.
WE ARE SASE.

Cato SASE Cloud Platform

Extended Detection and Response (XDR)
AI/ML-driven Anomaly Detection • Analyst Workbench with Gen-AI Stories • Incident Lifecycle Management

High-throughput Traffic Processing
Any Edge • Any Port/Protocol • DEM
Acceleration and Optimization • Selective Decryption

Threat Prevention and Data Protection
FWaaS • SWG • IPS • DNS • NGAM
ZTNA • CASB • DLP • RBI • IoT/OT

Single Management and API
- Granular RBAC
- Rich network and security analytics
- Automated Posture Management
- Self-service and Co-managed

SaaS Optimization
Smart Egress • Dedicated IP

Cato PoP
Single Pass Cloud Engine
SPACE

Multi Cloud Integration
Cato vSocket • Cloud interconnect • IPsec

aws

Global Private Backbone

Cato Socket Edge SD-WAN
A/A/A • Path Selection • App/Id Aware QoS • LAN Segmentation

MPLS

Clientless
via Web Portal

Cato Client
Universal ZTNA • EPP/EDR

Cato Client
Universal ZTNA • EPP/EDR

IoT

Use Cases

Network Transformation
MPLS to SD-WAN Migration

Global Access Optimization

Hybrid Cloud and Multi-Cloud Integration

Business Transformation
Vendor Consolidation

Spend Optimization

M&A and Geo Expansion

Security Transformation
Secure Hybrid Work

Secure Direct Internet Access

Secure Application and Data Access

Incident Detection and Response

Cato SASE Cloud Platform

Connect
Cloud Network

Cloud On-Ramps

Protect
Network Security

Endpoint Security

Detect
Incident Life Cycle Management

Run
Unified Management and API

CATO
NETWORKS

Contact Us